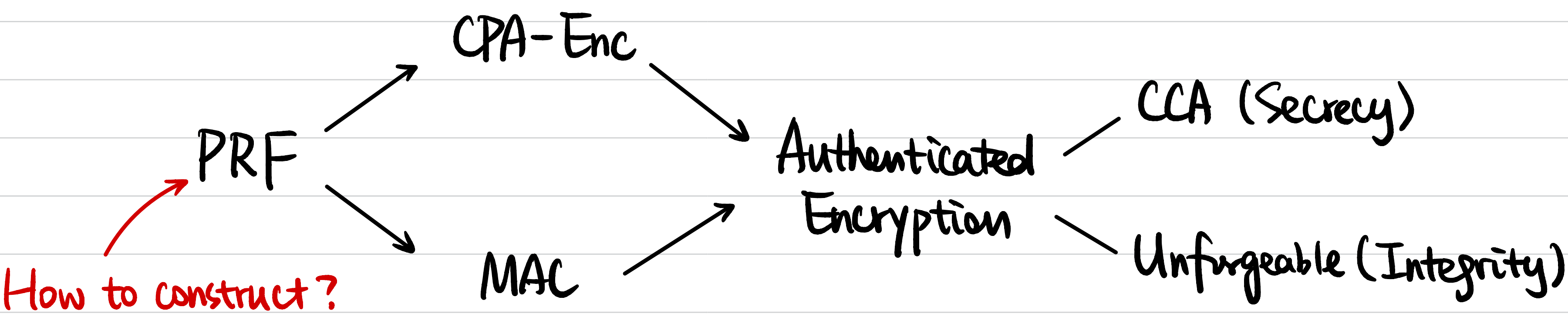
CSCI 1510

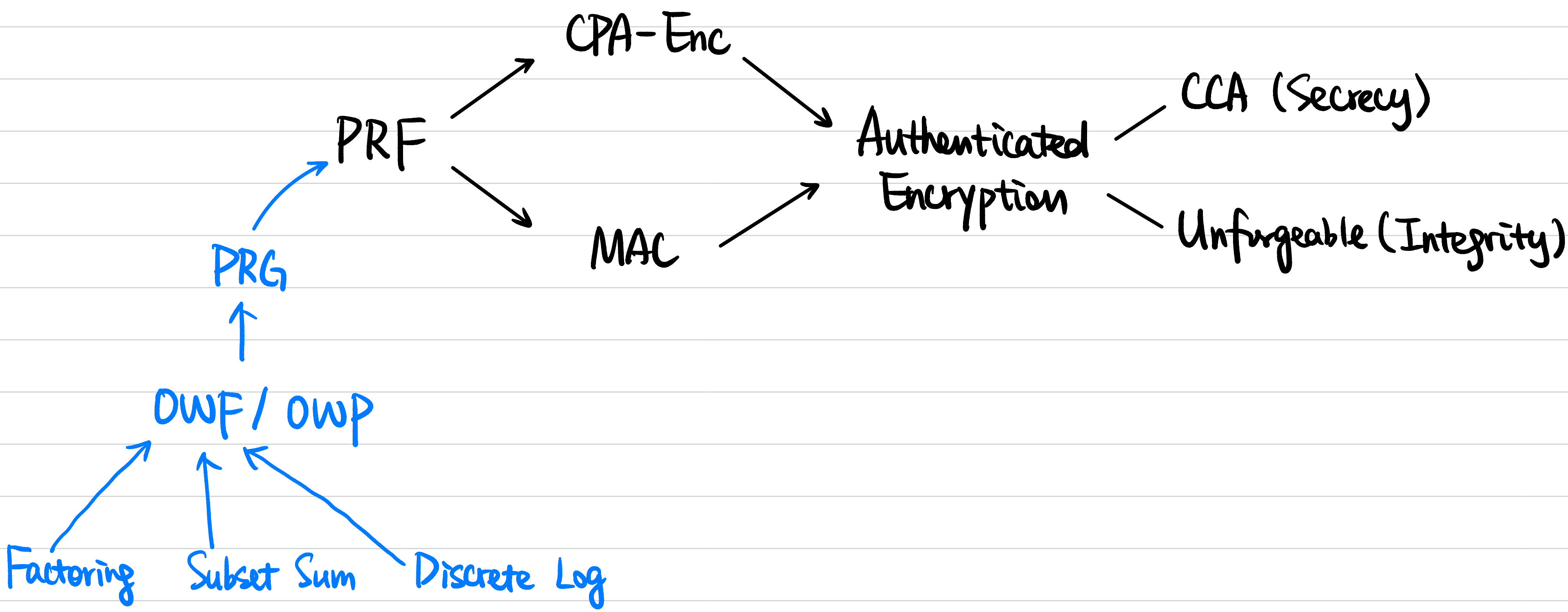
This Lecture:

- One-Way Function
- Hard-Core Predicate / Bit
- PRG from OWP



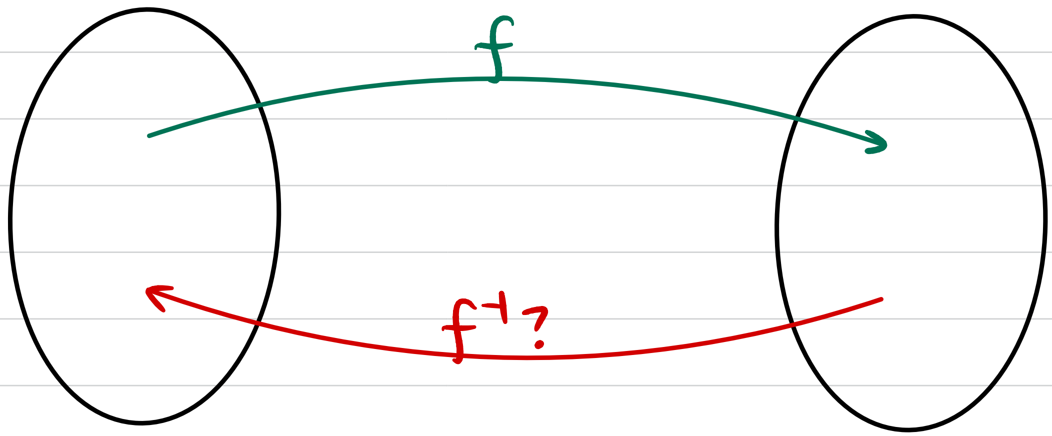
Practical Constructions: Block Cipher

Theoretical Constructions: from One-Way Function (OWF)


CPA-Enc
PRF
Authenticated Encryption
CCA (Secrecy)
Unforgeable (Integrity)
MAC
PRG
OWF / OWP
Factoring
Subset Sum
Discrete Log

One-Way Function

$f: \{0,1\}^* \to \{0,1\}^*$ that is easy to compute & hard to invert.



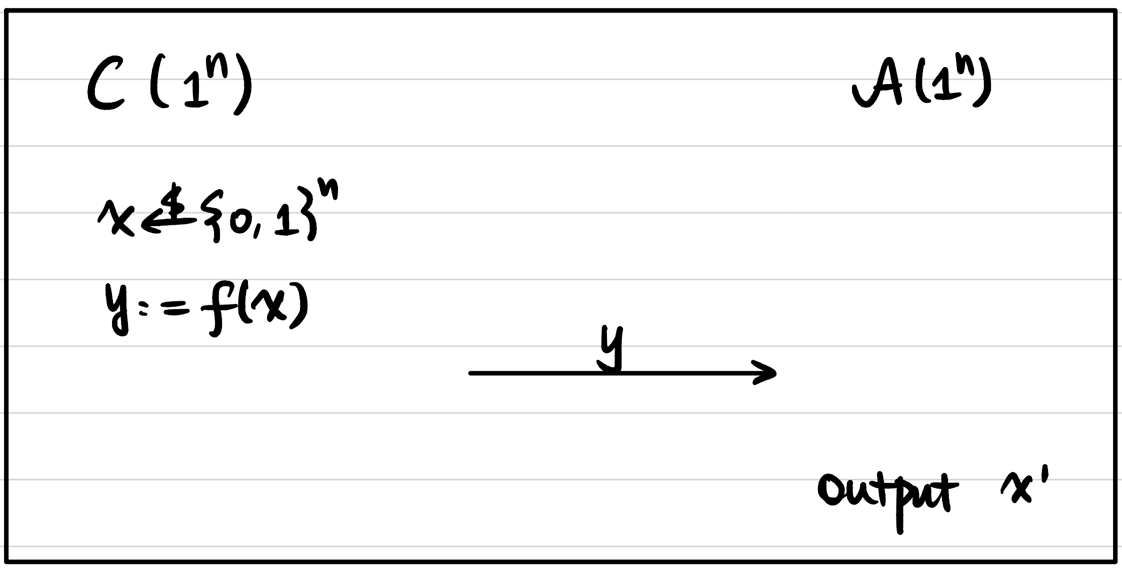
One-Way Function

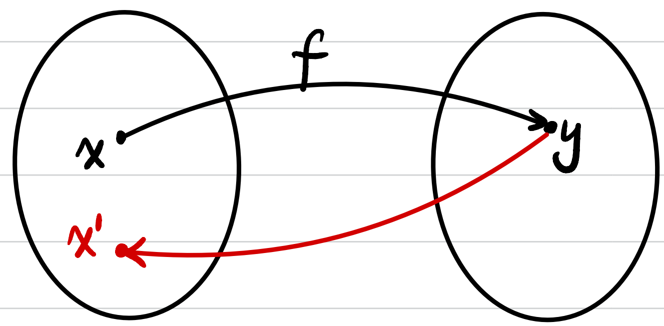
Def A function $f: \{0,1\}^* \to \{0,1\}^*$ is a **one-way function (OWF)** if

- easy to compute: $\exists$ poly-time algorithm M_f computing f. $\forall x$. $M_f(x) = f(x)$.
- hard to invert: $\forall$ PPT $\mathcal{A}$, $\exists$ negligible function $\varepsilon(\cdot)$ s.t.

$$\Pr_{x \xleftarrow{\$} \{0,1\}^n} [\mathcal{A}(1^n, f(x)) \in f^{-1}(f(x))] \le \varepsilon(n)$$

One-way permutation (OWP): $\{0,1\}^n \to \{0,1\}^n$, bijective.





$$\Pr[f(x') = y] \le \varepsilon(n).$$

What if $\mathcal{A}$ is computationally unbounded?

Candidate One-Way Functions

- **Factoring:** $f(x, y) = x \cdot y$

  ↑ x, y are n-bit primes

- **Subset Sum:** $f(x_1, x_2, \cdots, x_n, J) = (x_1, x_2, \cdots, x_n, \sum_{j \in J} x_j \bmod 2^n)$

  ↑
  $x_i \in \{0,1\}^n$ interpreted as an integer
  $J \in \{0,1\}^n$ interpreted as a subset of $[n]$

- **Discrete Log:** $f_{p,g}(x) = g^x \bmod p$

  ↑
  p is an n-bit prime.
  g is a "generator" for $\mathbb{Z}_p^*$.

- **SHA-2 / AES**

Exercises: Is g necessarily a OWF?

Let $f: \{0,1\}^n \to \{0,1\}^n$ be a OWF.

① $g(x) = \begin{cases} x & \text{if } x = 0^n \\ f(x) & \text{otherwise} \end{cases}$

② $g(x, y) = f(x) \| y \quad (|x| = |y|)$

③ $g(x) = f(x)[1 \ldots n-1]$ (least significant bit truncated)

Let $h: \{0,1\}^{n/2} \to \{0,1\}^{n/2}$ be a OWF.

$$f(x,y) = \begin{cases} x \,\|\, 0^{n/2-1} \,\|\, 1 & \text{if } y = 0^{n/2} \\ h(x) \,\|\, 0^{n/2} & \text{otherwise} \end{cases}$$

$$g(x,y) = \begin{cases} x \,\|\, 0^{n/2-1} & \text{if } y = 0^{n/2} \\ h(x) \,\|\, 0^{n/2-1} & \text{otherwise} \end{cases}$$

Step 1: f is a OWF.

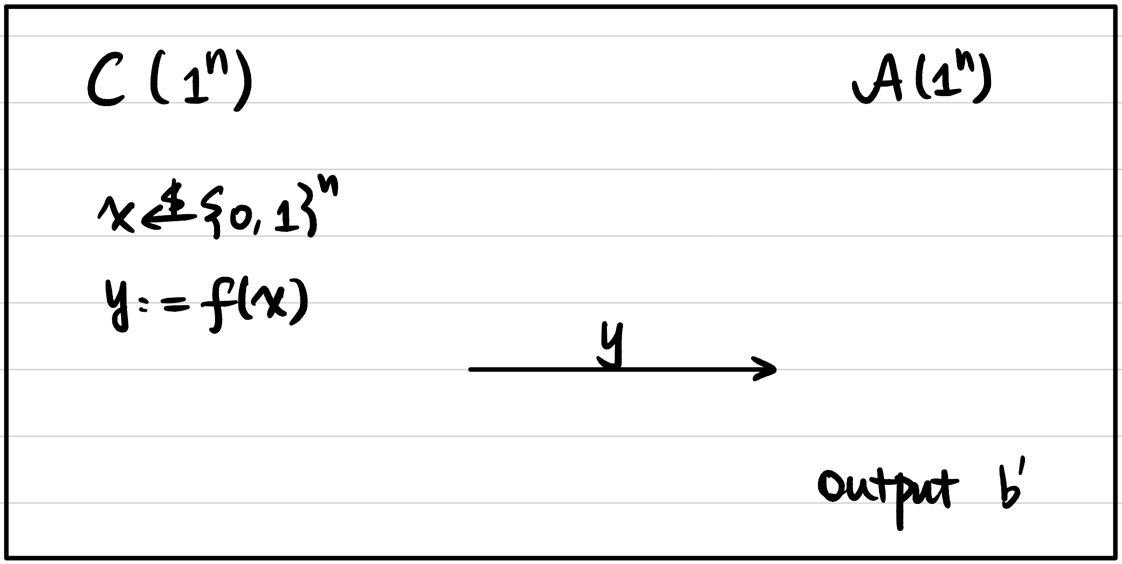
Step 2: g is not a OWF.

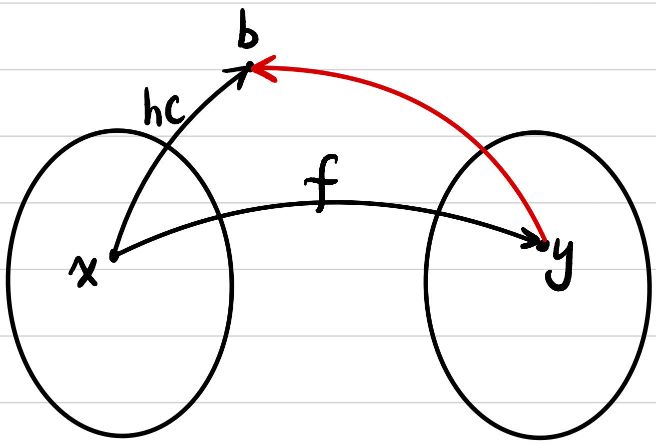
Hard-Core Predicate / Bit

Def A function $hc: \{0,1\}^* \to \{0,1\}$ is a hard-core predicate / bit of a function f if

- hc can be computed in poly time
- $\forall$ PPT $\mathcal{A}$, $\exists$ negligible function $\varepsilon(\cdot)$ s.t.

$$\Pr_{x \xleftarrow{\$} \{0,1\}^n} [\mathcal{A}(1^n, f(x)) = hc(x)] \le \frac{1}{2} + \varepsilon(n)$$





$\Pr[hc(x) = b'] \le \frac{1}{2} + \varepsilon(n)$.

Does every OWF have a hard-core predicate?

Constructing Hard-Core Predicate

Thm (Goldreich-Levin) Assume OWFs (resp. OWPs) exist.
Then there exists a OWF (resp. OWP) g and a hard-core predicate hc of g.

Given a OWF f, (OWP)

Construct another OWF (OWP) $g(x, r) := (f(x), r)$, $|x| = |r|$.

with a hard-core predicate $hc(x, r) := \bigoplus_{i=1}^{n} x_i \cdot r_i$

Thm hc is a hard-core predicate of g.

Proof Assume not, then $\exists$ PPT $\mathcal{A}$ that breaks the hard-core predicate hc. ← with probability 1.
We construct a PPT $\mathcal{B}$ to break the one-wayness of f.

Constructing PRG from OWP

Let $g : \{0,1\}^n \to \{0,1\}^n$ be a OWP with hard-core predicate hc.

Construct $G : \{0,1\}^n \to \{0,1\}^{n+1}$

$$G(s) = g(s) \,\|\, hc(s).$$

Thm G is a PRG.

Increasing the Expansion